Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2014–2015

33 662

Wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp)

B

VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR VEILIGHEID EN JUSTITIE[1]

Vastgesteld 17 maart 2015

Het voorbereidend onderzoek heeft de commissie aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

1. Inleiding

De leden van de **VVD**-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij zijn van mening dat dit wetsvoorstel een belangrijke bijdrage kan leveren aan het verbeteren van de informatiebeveiliging van veel organisaties die onder de Wet bescherming persoonsgegevens (hierna: Wbp) vallen, als ook aan het verbeteren van de bescherming van de persoonlijke levenssfeer van betrokkenen. Deze leden hebben nog een aantal vragen.

De leden van de **PvdA**-fractie hebben met instemming kennisgenomen van het wetsvoorstel. Zij kunnen zich vinden in de aan het Cbp geboden mogelijkheid om een bestuurlijke boete op te leggen bij het niet melden van datalekken. Ook vinden zij het wijs dat het opleggen van een dergelijke boete in de meeste gevallen voorafgegaan moet worden door een (bindende) aanwijzing. Zeker omdat – en hier hebben de meeste

[1] Samenstelling:
Holdijk (SGP), Kneppers-Heijnert (VVD), Kox (SP), Engels (D66), Franken (CDA), Thissen (GL), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA) *(vice-voorzitter)*, Duthler (VVD) *(voorzitter)*, Koffeman (PvdD), Kuiper (CU), Quik-Schuijt (SP), Strik (GL), De Vries (PvdA), Knip (VVD), Hoekstra (CDA), Lokin-Sassen (CDA), Scholten (D66), Schouwenaar (VVD), De Boer (GL), De Lange (OSF), Ter Horst (PvdA), Beuving (PvdA), Koole (PvdA), Schrijver (PvdA), Reynaers (PVV), Popken (PVV), Frijters-Klijnen (PVV), Swagerman (VVD)

kst-33662-B
ISSN 0921 - 7371
's-Gravenhage 2015

vragen betrekking op – niet geheel klip en klaar is wanneer een datalek aan het Cbp en/of betrokkenen moet worden gemeld en wanneer niet.

De leden van de **CDA**-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij onderschrijven het doel van de voorgestelde meldplicht en van andere meldplichten met betrekking tot datalekken of andere ernstige incidenten met betrekking tot de bedrijfsvoering. Zij zien als dit doel het vergroten van het vertrouwen van het publiek in digitale gegevensverwerking. Daarnaast moet het met behulp van de voorgestelde bepalingen mogelijk zijn om lessen te leren van opgetreden datalekken. Wel is in verband met de effectiviteit van het toezicht en de handhaving een geclausuleerde omschrijving van de door de burger na te leven plicht noodzakelijk. Deze leden stellen evenwel vast dat, ondanks dat de titel van het wetsvoorstel anders doet vermoeden, de wettelijke bepalingen alleen betrekking hebben op een doorbroken beveiliging.
De aan het woord zijnde leden zullen zich na de uitgebreide behandeling in de Tweede Kamer en de naar aanleiding daarvan aangebrachte veranderingen beperken tot slechts nog enkele vragen.

De leden van de **SP**-fractie hebben met gemengde gevoelens kennisgenomen van het wetsvoorstel. Tien jaar geleden nam de Tweede Kamer de motie-Gerkens/Van Dam[2] aan die de regering opriep tot het instellen van een meldplicht. Het heeft lang geduurd, veel te lang, voordat deze motie is omgezet in een wetsvoorstel. Dat het wetsvoorstel er nu daadwerkelijk is, verheugt deze leden dan ook zeker. Het is een stap vooruit en de maatregel kan rekenen op een groot draagvlak, zo getuige ook de behandeling in de Tweede Kamer.
Met dit wetsvoorstel geeft de overheid een duidelijk signaal af: persoonsgegevens dienen goed beveiligd te worden. Maakt men hier geen serieus werk van en gaat er iets mis, dan kan het College bescherming persoonsgegevens (hierna: Cbp) stevige boetes uitdelen. De door de Tweede Kamer aangenomen amendementen verbeteren het wetsvoorstel door de mogelijkheden van het Cbp verder te versterken.
Maar zal dit wetsvoorstel uiteindelijk de positie van de consument verbeteren? Vooral op dit punt willen de leden van de SP-fractie een aantal vragen stellen en opmerkingen maken. Daarbij sluiten de leden van de fractie van **GroenLinks** zich aan.

De leden van de **D66**-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel dat onder meer een meldplicht invoert bij een inbreuk op beveiliging van persoonsgegevens en het Cbp meer bevoegdheden geeft om bij die inbreuk bestuurlijk op te treden door de bestuurlijke boete in te voeren. Deze leden hebben een enkele vraag.

2. Strekking van het wetsvoorstel

De indieners van de motie-Gerkens/Van Dam hadden een bredere meldplicht voor ogen dan nu wordt voorgesteld. De consument zou volgens hen altijd op de hoogte moeten worden gesteld als er een inbreuk heeft plaatsgevonden. De regering en de Europese instellingen kiezen ervoor dit niet te doen. Het zou dan zoveel meldingen geven dat het effect van de meldplicht teniet zou worden gedaan. De leden van de **SP**-fractie beamen dit, wanneer de melder altijd melding zou moeten doen bij het Cbp. Maar deze leden zijn van mening dat een ieder het recht heeft om te weten of zijn of haar gegevens wellicht bij iemand gestolen kunnen zijn. Dat is nodig om maatregelen te kunnen treffen om te voorkomen dat met de gegevens onrechtmatige handelingen zouden kunnen worden gedaan.

[2] *Kamerstukken II* 2005–2006, 26 671, nr. 20.

In Nederland zijn vele webwinkels die massa's gegevens vragen zonder een beveiligde verbinding te gebruiken. Toen de vereniging HCC een meldpunt hierover opende, kwamen er zelfs meldingen binnen van onbeveiligde pagina's van een grote pensioenuitvoerder die de complete overdrachtsgegevens van verzekerden en hun partners over een niet-beveiligde lijn liet invullen. Kinderdagverblijven hadden online inschrijfformulieren en zorgverzekeraars hadden contactformulieren met burgerservicenummers die niet beveiligd waren. HCC nam iedere keer contact op met het bedrijf met het verzoek de pagina's te beveiligen. Daaruit bleek dat veel ondernemers gewoonweg niet wisten dat deze beveiligd dienen te zijn. Zo gaven veel ondernemers aan dat ze hun website door een professioneel bedrijf hadden laten maken en dat «het dus wel goed zou zitten» of men reageerde met de opmerking dat naam, adres, geboortedatum en telefoonnummer geen persoonsgegevens zijn. Bewustwording op dit gebied bij deze ondernemers is nog heel ver te zoeken. De consument wordt daar de dupe van. Zijn of haar gegevens zijn heel eenvoudig te achterhalen. Helaas is de consument zelf zich daar ook te weinig van bewust. Anders zou deze er vaker voor kiezen om de gegevens niet in te vullen en op zoek te gaan naar een andere aanbieder. Wat gaat de regering doen om de bewustwording op dit gebied te verhogen?
Zelfs goedwillende ondernemers, die maatregelen treffen, kunnen gehackt worden. En dan is een boete niet het meest belangrijke, maar het informeren van de betrokkenen wel. De leden van de SP-fractie willen de volgende situatie aan de regering voorleggen om dit te illustreren. Afgelopen zomer werd er ruim een miljard gegevens buitgemaakt op internet. In oktober bleek dat hier een ruim miljoen e-mailadressen en inloggegevens, inclusief wachtwoorden, van Nederlanders tussen zaten. Het Nationaal Cyber Security Centrum (NCSC), dat onderdeel is van het Ministerie van Veiligheid en Justitie, heeft vervolgens contact gehad met de internetproviders waar de Nederlandse e-mailadressen onder vallen. De providers *konden* getroffen gebruikers informeren dat ze slachtoffer waren geweest van de hack. «Mensen in het bezit van een e-mailadres eindigend op.nl die geen bericht van hun provider ontvangen, kunnen er over het algemeen van uitgaan dat hun e-mailadres geen onderdeel is van deze dataset», schreef het NCSC. Hoe de providers hiermee omgingen, was wisselend. Via de media berichtte XS4all dat men via een tool op de website kon zien of een e-mailadres erbij betrokken was. Als dat het geval was, was het advies om alle wachtwoorden op websites te wijzigen. Vandaag de dag hebben mensen echter ontelbare wachtwoorden op ontelbare websites. Het is ondoenlijk om die allemaal te wijzigen, laat staan om te weten welke sites het allemaal zijn. Sommige zijn van jaren geleden, sommige hebben wel betaalgegevens, andere niet. Soms is het een inschrijving op een nieuwsbrief. Kortom, al zou men op alle websites het wachtwoord wijzigen, dan weet men nog niet of dit gehackte websites betreffen. De NCSC geeft aan dat ze de namen van de websites niet wil geven in verband met reputatieschade. Een betrokkene moet dus maar hopen dat de website hem of haar waarschuwt, maar de website hoeft dat niet te doen. Resultaat is dat er niets gebeurd. Dat is naar de stellige overtuiging van de leden van de SP-fractie precies waar het probleem zit en ook blijft. Is de regering het met deze leden eens dat hiermee het grootste probleem van datalekken nog niet ondervangen is? Wetende dat geen enkele website ooit 100% veilig kan zijn, is dan de angst voor reputatieschade niet onterecht, en sterker nog, is de bescherming van de goede naam niet in strijd met de bescherming van de privacy en veiligheid op internet?
Is de regering het met de aan het woord zijnde leden eens dat idealiter bedrijven hun klanten zelf actief informeren bij een mogelijk datalek? Op deze wijze kan de klant zelf stappen ondernemen om zijn wachtwoord te wijzigen. Is de regering het met deze leden eens dat dit zeker moet

gebeuren bij ieder lek waar ook financiële gegevens zijn buitgemaakt? Zo ja, op welke wijze wil de regering zich hiervoor inzetten? De leden zouden zich kunnen voorstellen dat een dergelijke informatieplicht eerst op basis van zelfregulering kan worden geïntroduceerd. Graag een reactie van de regering.

3. Beleidsmatige achtergrond

3.1 Verhouding met Europese wetgevingsvoorstellen

De leden van de **VVD**-fractie zouden graag van de regering vernemen hoe het wetsvoorstel zich verhoudt tot het wetsontwerp dat onlangs in consultatie is gegaan en dat een implementatie beoogt van de voorgestelde richtlijn Netwerk- en Informatiebeveiliging (COM(2013)48), die reeds in eerste lezing door het Europees parlement is aangenomen? In dit wetsontwerp is ook een meldplicht datalekken opgenomen, die weliswaar breder is maar ook betrekking kan hebben op de in het onderhavige wetsvoorstel bedoelde datalekken. Hoe is de samenloop? Kan het zo zijn dat verantwoordelijken zowel moeten melden aan het Cbp als aan de in het wetsontwerp genoemde autoriteit? Hoe wordt voorkomen dat een verantwoordelijke zowel een boete opgelegd kan krijgen door het Cbp als gevolg van het niet onverwijld melden als door een andere toezichthouder?

Met het wetsvoorstel wordt voor een belangrijk deel vooruitgelopen op de totstandkoming van de Algemene verordening gegevensbescherming (COM(2012)11) en de richtlijn voor de bescherming van persoonsgegevens in de sectoren van politie en justitie (COM(2012)10), die de huidige EU-privacyrichtlijn uit 1995 zullen vervangen. Hoewel de onderhandelingen over deze documenten nog in volle gang zijn – de regering sprak in de nota naar aanleiding van het verslag de verwachting uit dat deze in 2015 zal tot stand komen en in werking treden – zouden de leden van de **CDA**-fractie graag vernemen welke aanpassingen met betrekking tot de onderwerpen, die in dit wetsvoorstel aan de orde zijn, naar aanleiding van deze Europese regelgeving mogen worden verwacht.

3.2 Verhouding tot andere meldplichten die betrekking hebben op de bedrijfsvoering in de private of publieke sector

De leden van de **CDA**-fractie stellen het op prijs om een beknopt maar geheel geactualiseerd overzicht te krijgen van de diverse meldplichten die betrekking hebben op datalekken of andere ernstige incidenten met betrekking tot de bedrijfsvoering van bedrijven en van de overheid, die thans gelden of binnen afzienbare tijd in Europese wetgeving zullen worden vastgesteld. Dit overzicht zou in ieder geval de na te noemen categorieën moeten bevatten: de wettelijke basis, de adressaat van de norm, de mogelijke sancties, de bevoegdheid van de toezichthouder(s) en de mogelijkheden van rechtsbescherming.

4. Algemene aspecten van de meldplicht

In het voorgestelde artikel 34a, vijfde lid, wordt bepaald dat de kennisgeving aan betrokkenen van datalekken op zodanige wijze wordt gedaan dat een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd. De leden van de **VVD**-fractie vragen de regering om voorbeelden te geven wanneer wel en wanneer niet sprake is van zo'n behoorlijke en zorgvuldige informatievoorziening. Ook vernemen zij graag of de verantwoordelijke, als sprake is van tienduizenden of meer betrokkenen, kan volstaan met een algemene kennisgeving in verschillende media. Of moeten ook dan alle betrokkenen individueel worden geïnformeerd?

Op grond van het achtste lid van artikel 34a is de verantwoordelijke verplicht om een overzicht bij te houden van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Dient de verantwoordelijke een dergelijk overzicht ook openbaar te maken? En hoe lang dient een dergelijk overzicht bewaard te blijven? De aan het woord zijnde leden verzoeken de regering op deze vragen te reageren.
Het Cbp zal de meldingen vertrouwelijk behandelen, zo wordt in de memorie van toelichting aangegeven. Het Cbp is een zelfstandig bestuursorgaan en valt als zodanig onder de Wet openbaarheid van bestuur (Wob). Dit kan ondernemingen in een spagaat brengen. Melden zij een hack wel bij het Cbp, dan lopen zij mogelijk schade. Melden zij niet, dan krijgen ze mogelijk een boete opgelegd door het Cbp. Welke waarborgen biedt de Wob op dit punt, zo willen de leden van de VVD-fractie van de regering weten.

Als het gaat om de vraag hoe de meldplicht op zinvolle wijze kan worden beperkt, verwijst de regering naar de regelgeving in Duitsland en Oostenrijk waar een veel specifiekere omschrijving wordt gegeven van de datalekken die in aanmerking komen voor melding dan in het huidige wetsvoorstel wordt gehanteerd. Is de regering met de leden van de **PvdA**-fractie van mening dat de gekozen omschrijving – aanzienlijke kans op ernstig nadelige gevolgen – niet eenduidig is en voor organisaties problemen kan opleveren bij het beoordelen of zij een datalek moeten melden of niet? Acht de regering de verwachting reëel dat organisaties/instellingen als beleidslijn «better safe than sorry» zullen kiezen en vaker dan nodig is datalekken zullen melden? En zou daar dan niet juist de situatie kunnen ontstaan die de regering wil voorkomen, zoals aangegeven in haar reactie op het voorstel van Bits of Freedom, namelijk dat te veel en te vaak overbodig wordt gemeld? Kan de regering aangeven of zij het verantwoord vindt dat de interpretatie van de omschrijving wanneer gemeld moet worden bij de verantwoordelijke voor het datalek ligt en niet bij de wetgever?
In ditzelfde kader zouden de aan het woord zijnde leden graag van de regering vernemen of hacken nu wel of niet tot melding moet leiden. In de memorie van toelichting zegt de regering dat het hacken van een ICT-systeem wel in de categorie te melden datalekken valt, maar het hacken uit de zienswijze van Bits of Freedom niet. Kan de regering aangeven hoe dit precies zit?
In de memorie van toelichting wordt de meldplicht opgevat als een administratieve verplichting. Hieruit spreekt de suggestie dat de regering de beoordeling of gemeld moet worden opvat als een simpele, digitale beoordeling. Klopt dit inderdaad of wenst de regering deze suggestie weg te nemen?

Hoewel ook bij de behandeling in de Tweede Kamer de «onbepaaldheid» van de wettelijke verplichting voor de burger uitgebreid is ter sprake gekomen, is het voor de leden van de **CDA**-fractie nog niet volstrekt helder hoe deze norm voldoende duidelijk, voorzienbaar en kenbaar zal zijn (lex certa beginsel). Het is immers voor bedrijven en overheden van belang om aan de hand van feiten en omstandigheden van het concrete geval te kunnen beoordelen of een datalek binnen het bereik van de meldingsplicht valt. De voorgestelde oplossing is dat het Cbp door middel van richtsnoeren een nadere verduidelijking zal geven. Deze richtsnoeren (beleidsregels) zouden dan volgens het voorgestelde, bij nota van wijziging ingevoegde, artikel 67 na overleg met de Ministers van Veiligheid en Justitie en van Binnenlandse Zaken en Koninkrijksrelaties worden vastgesteld.
Deze procedure is op papier duidelijk, maar het blijft voor de burger moeilijk om te weten wanneer er van een relevante inbreuk op een

beveiliging sprake is. Het gaat dan niet aan om – zoals de regering doet – te volstaan met een verwijzing naar het feit dat de normstelling in de Wbp nu eenmaal als algemeen-abstract kan worden gekenschetst in verband met de grote diversiteit aan verwerkingen van persoonsgegevens in de private en publieke sector. Bovendien zal hier een groot verschil zijn wanneer een relatief kleine inbreuk plaatsvindt bij een particuliere vereniging of een kleine onderneming dan wel bij een overheidsinstelling als de Belastingdienst of de Sociale Verzekeringsbank. Kortom, een catalogus van richtsnoeren zal wel tot het kennispakket van een overheidsinstantie behoren, maar dit kan van een ZZP-er niet zonder meer worden gevraagd. Deze aanpak leidt tot de aanzienlijke kans dat het Cbp uit angst voor formidabele boetes met veel onnodige c.q. onterechte meldingen zal worden geconfronteerd of juist dat de burgers wegens de onduidelijkheid van de normstelling schouderophalend aan «het hele gedoe» zullen voorbijgaan. Gaarne vernemen de aan het woord zijnde leden het standpunt van de regering hieromtrent.

5. Sanctionering

In de toelichting op de tweede nota van wijziging wordt gesproken over de figuur van medepleger als bedoeld in de Algemene wet bestuursrecht (hierna: Awb). Dit kan zijn een bewerker in de zin van de Wbp maar ook een feitelijk opdrachtgever of een feitelijk leidinggevende. Betekent dit dat bijvoorbeeld een afdelingshoofd of manager die feitelijk verantwoordelijk is voor een bepaalde gegevensverwerking ook een boete opgelegd kan krijgen als bedoeld in het wetsvoorstel? En kunnen de feitelijk leidinggevende en verantwoordelijke in bijvoorbeeld hun arbeidsovereenkomst vastleggen of anderszins overeenkomen dat in voorkomende gevallen de verantwoordelijke de feitelijk opdrachtgever of leidinggevende compenseert ter waarde van de hoogte van de boete? De leden van de **VVD**-fractie vernemen graag de reactie van de regering op deze vragen.

Ten aanzien van de hoogte van de boete als percentage van de omzet (maximaal 10%) vragen de leden van de **PvdA**-fractie zich af of het niet in geld maximeren van deze boete niet heel veel ruimte aan het Cbp geeft. En, zo willen deze leden weten, heeft de regering de consequenties van een dergelijke boete voor een bedrijf overwogen? Is de regering bereid een maximumbedrag vast te stellen teneinde onwenselijke consequenties te voorkomen?
De Afdeling advisering van de Raad van State (hierna: Afdeling) vroeg de regering of het instrument van (bestuurlijke) strafbaarstelling overwogen is. De regering reageerde daarop door te stellen dat dit instrument naast de bestuurlijke boete geen meerwaarde heeft en het systeem zou compliceren. Naar de mening van de aan het woord zijnde leden was de intentie van de Raad van State om te informeren naar de (bestuurlijke) strafbaarstelling in plaats van de bestuurlijke boete, niet ernaast. De leden verzoeken de regering deze vraag alsnog te beantwoorden.
De Afdeling heeft voorts de vraag opgeworpen of de bestuurlijke boete en niet strafbaarstelling het geëigende punitieve middel is. De leden vragen de regering om de belangrijkste argumenten voor deze principiële keuze kenbaar te maken.
De Afdeling heeft daarnaast op de mogelijkheid gewezen dat in de op handen zijnde Algemene verordening gegevensbescherming (COM(2012)11) bepaalde feiten wellicht niet in aanmerking komen voor een bestuurlijke boete. Hoewel de leden van de PvdA-fractie er begrip voor hebben dat de regering niet op de EU-verordening heeft gewacht voordat zij met eigen voorstellen kwam, zouden zij graag een beoordeling van de regering willen zien van de kans waar de Afdeling op doelt.

Naast de bestuurlijke boete kan het Cbp ook een bindende aanwijzing geven. Het Cbp kan deze bindende aanwijzing, gevolgd door een boete, opleggen in een aantal in de Wbp genoemde gevallen, waaraan in dit wetsvoorstel wordt toegevoegd de mogelijkheid tot het geven van een bindende aanwijzing in geval van een vermoeden van inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, aldus de tekst van het voorgestelde artikel 34a.
Dit artikel is als algemeen abstracte norm geformuleerd. Vanwege het lex certa beginsel vragen de leden van de **D66**-fractie of de regering voorbeelden kan geven van inbreuken die in het concrete geval zullen vallen onder het toepassingsbereik van genoemd artikel, voorbeelden die betrekking hebben op inbreuken die leiden tot de aanzienlijke kans op ernstige nadelige gevolgen als ook voorbeelden die betrekking hebben op inbreuken die ernstige nadelige gevolgen tot gevolg hebben.
De bindende aanwijzing is bedoeld om de vermoedelijke overtreder op het rechte pad te houden en om hem te dwingen de vermoedelijke inbreuk geheel of gedeeltelijk te herstellen. Is hier voorzien in rechtsbescherming van de vermoedelijke overtreder? Kunnen de beschermingsbepalingen van de Awb onverkort worden toegepast in geval van bezwaar en beroep tegen een bindende aanwijzing?

6. Concentratie van taken bij het Cbp

Ten aanzien van de totstandkoming van nadere normstelling nam de regering het advies van de Afdeling over om de Minister van Veiligheid en Justitie te laten instemmen met de richtsnoeren van het Cbp. Echter, de Tweede Kamer was vervolgens van mening dat dit onwenselijk is omdat de rijksoverheid ook onder de wet valt en had een voorkeur voor overleg tussen het Cbp en de Ministers van Veiligheid en Justitie en van Binnenlandse Zaken en Koninkrijksrelaties. Het aangenomen amendement onder volgnummer 22 realiseert deze aanpassing. De Afdeling had nog een tweede mogelijkheid genoemd, namelijk om die nadere invulling bij algemene maatregel van bestuur (hierna: AMvB) te laten plaatsvinden. De leden van de **PvdA**-fractie kunnen zich voorstellen dat dat een goed alternatief zou zijn. Zij zouden dan ook graag van de regering vernemen of het alternatief van de AMvB door de regering alsnog overwogen is en zo ja, wat de argumenten zijn geweest om dit niet aan de Tweede Kamer voor te leggen.

7. Tot slot

Het Cbp zal, als het onderhavige wetsvoorstel is aangenomen, verder de naam dragen «Autoriteit Persoonsgegevens». Bij de leden van de **CDA**-fractie is de vraag gerezen of deze benaming wel recht doet aan de taken die het Cbp uitoefent. Het lijkt toch juist de beschermingsfunctie te zijn die de kern vormt van het bestaan van dit college. Gaarne een reactie.

De leden van de vaste commissie voor Veiligheid en Justitie zien de reactie van de regering – bij voorkeur binnen vier weken – met belangstelling tegemoet.

De voorzitter van de vaste commissie voor Veiligheid en Justitie,
Duthler

De griffier van de vaste commissie voor Veiligheid en Justitie,
Van Dooren